UNITED STATES DISTRICT COURT

DISTRICT OF ARIZONA

In Re: Search Warrant For: 621 S. 48th Street, Suite 114, Tempe, Arizona 85281	13-6280MB **ORDER** (Filed Under Seal)

Based upon the Motion of the United States of America, and good cause appearing,

IT IS ORDERED that the Application and Affidavit for the Search Warrant, and the Motion to Seal and this Order are hereby sealed on the grounds that disclosure would jeopardize an ongoing investigation and should remain sealed until further order of this Court.

DATED this 26th day of Apr., 2013.

HONORABLE DAVID K. DUNCAN
United States Magistrate Judge

JOHN S. LEONARDO
United States Attorney
District of Arizona

JENNIFER LEVINSON
Assistant U.S. Attorney
Arizona State Bar No. 020551
Two Renaissance Square
40 N. Central Avenue, Suite 1200
Phoenix, Arizona 85004-4408
Telephone: (602) 514-7500
Jennifer.Levinson@usdoj.gov

UNITED STATES DISTRICT COURT

DISTRICT OF ARIZONA

In Re:

Search Warrant For:

621 S. 48th Street, Suite 114,
Tempe, Arizona 85281

13-6280MB

MOTION TO SEAL SEARCH WARRANT APPLICATION AND AFFIDAVIT

(Filed Under Seal)

The United States of America moves this Court for an Order sealing the Application and Affidavit for the Search Warrant, and the Motion to Seal and the Order to Seal in this matter, on the grounds that disclosure would jeopardize an ongoing investigation.

Respectfully submitted this 26th day of April, 2013.

JOHN S. LEONARDO
United States Attorney
District of Arizona

JENNIFER LEVINSON
Assistant United States Attorney

UNITED STATES DISTRICT COURT

for the

District of Arizona

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

621 S. 48th Street, Suite 114,
Tempe, Arizona 85281

Case No. 13-6280MB

SEALED

APPLICATION FOR A SEARCH WARRANT

I, Richard Langley, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*
SEE ATTACHMENT A incorporated herein by reference.

located in the _____ District of Arizona, there is now concealed *(identify the person or describe the property to be seized)*:
SEE ATTACHMENT B incorporated herein by reference

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Sections	*Offense Description*
18 U.S.C. § 545	Smuggling
18 U.S.C. § 542	False Declarations
21 U.S.C. §§ 333(a)(1) & (2)	Violations of the FDCA

The application is based on these facts:

SEE ATTACHED AFFIDAVIT INCORPORATED BY REFERENCE HEREIN.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Authorized by AUSA Jennifer Levinson

_____
Applicant's signature

Richard Langley, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: Apr. 26, 2013

_____
Judge's signature

City and state: Phoenix, Arizona

Honorable David K. Duncan, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

Property to be searched

The property to be searched is the business office of CBSChem Limited located in the Airport Business Center at 621 S. 48th Street, Suite 114, Tempe, AZ 85281. The property is attached to and part of a larger one-story building identified as 621 S. 48th Street, Tempe, AZ 85281. The building is a one-story tan concrete and mirrored black glass building with rectangular vertical columns running along the outside.

Prominently displayed on the NE corner of the building up high on the Eastern facing side, in black lettering with a red swish line though the numbers "6" and "2" are the numbers "621". On the Eastern facing side of the building on a white background above a mirrored black glass door are the numbers "114", in black with a red swish line through the numbers "1" and "1". Located to the left of the door on the mirrored black glass is a dark blue sign with white lettering containing the word "cbsCHEM". A white line is also displayed under the word "cbsCHEM". Also located to the left of the door sticking out of the ground is a diamond shaped sign with the word "TITAN" on it. To the right of the door is a palm tree.

Attached is a photograph of the entrance to Suite 114 along with a layout of the Airport Business Center.

cbsCHEM

ATTACHMENT B

Items to be seized

1. For the time period of October 15, 2011 through the present, all records and information in any form, whether electronic or not, constituting evidence and/or instrumentalities of violations of: (1) 18 U.S.C. § 545 (smuggling); (2) 18 U.S.C. § 542 (false declarations); and (3) 21 U.S.C. § 333(a)(1)&(2) (violations of the Federal Food Drug and Cosmetics Act including introducing misbranded drugs into interstate commerce in violation of 21 U.S.C. § 331(a) and delivery of misbranded drugs for pay in violation of 21 U.S.C. § 331(c)), committed by KAMIRAN RAZA MALIK and CBS CHEM LIMITED and/or its employees. Such records and information include the following:

    a. Records associated with or pertaining to the smuggling, acquisition, possession and distribution of misbranded pharmaceuticals involving CBSCHEM Limited.
    b. Records related to the manufacturing, brokering, ordering, purchasing, shipping, sale and distribution of any misbranded pharmaceutical, including business journals and ledgers; tax records and related work papers; purchase and sales records; communications; pedigrees; bank and financial records; shipment/transport records; supplier and customer records; manufacturing records, certificates of analysis, laboratory analysis, regulatory compliance records and communications with federal, state and local authorities.

2. Any and all misbranded pharmaceuticals including Active Pharmaceutical Ingredients (APIs). This includes any packaging, labeling, import documentation or shipping materials that may accompany the pharmaceuticals.

3. Computers or storage media used as a means to commit the violations described above.

4. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

    a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. records of or information about Internet Protocol addresses used by the COMPUTER;

j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

k. contextual information necessary to understand the evidence described in this attachment.

5. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical,

arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

AFFIDAVIT

I, Richard Langley, being first duly sworn, hereby depose and state as follows:

AGENT BACKGROUND

1. I am a Special Agent with the United States Food and Drug Administration, Office of Criminal Investigations (FDA/OCI). I have been so employed in this capacity for two years. As a Special Agent with this agency, I am responsible for enforcing federal laws that pertain to the unlawful importation of controlled substances as listed under Title 21, United States Code, Section 841(a)(1) and 846, and enforcement of the Federal Food, Drug and Cosmetic Act as defined under Title 21 United States Code, Section 301. I am currently assigned to the FDA/OCI Domicile office, Phoenix, Arizona.

2. Prior to this current position, I was employed as a Special Agent for two years with the United States Immigration and Customs Enforcement and eight years as a Special Agent with the United States Secret Service. I have had extensive training in the Criminal Justice field and have studied many topics to include Criminal Investigations, Fourth Amendment, Law of Search and Seizure, and other laws and law enforcement techniques.

3. I have attended over thirty weeks of specialized training at the Federal Law Enforcement training Academy in Glynco, Georgia, twenty weeks of specialized training at the United States Secret Service Academy in Beltsville, Maryland, and hundreds of hours of additional refresher training in various settings. The training included undercover investigations, conspiracy law,

controlled substance trafficking, money laundering, patterns of drug distribution, drug identification, and electronic surveillance procedures. As a law enforcement officer, I have employed a variety of investigative techniques, including physical and electronic surveillance, undercover transactions, and execution of search warrants. I have spoken with numerous defendants, confidential informants, and witnesses having extensive knowledge of the workings of major narcotics trafficking organizations, as well as with other law enforcement personnel concerning the methods and practices of drug traffickers.

4. Through my investigations, training, experience, and discussions with other law enforcement personnel, I have become familiar with the tactics and methods used to import and distribute illegal pharmaceuticals and controlled substances. This includes tactics to distribute controlled substances and to collect and launder the proceeds from the sale of controlled substances. These tactics and methods include the use of cellular telephones, cloned communication devices, digital display paging devices, debit calling cards, public pay telephones, counter-surveillance techniques, false or fictitious identities, coded communications, and coded words in conversations. Through my experience and training, I have also become familiar with the methods used by foreign companies and others, to smuggle drugs and contraband into the United States via the mails. These methods commonly involve falsifying U.S. Customs Declaration documents to avoid inspection at the inbound mail facilities.

INTRODUCTION

5. The information contained in this affidavit is being offered for the limited purpose of this warrant application and does not encompass all of the information possessed by the government at this time.

6. I have personally been involved in the investigation of CBSCHEM LIMITED and the owner KAMRAN RAZA MALIK who is believed to be engaged in the introduction of misbranded pharmaceutical drugs into interstate commerce.

7. The following information is known by myself or has been provided to me by other regulatory and law enforcement officials.

RELEVANT STATUTES

Federal Food, Drug and Cosmetic Act

8. The Federal Food, Drug, and Cosmetic Act, 21 U.S.C. §§ 301 et seq. ("FDCA") regulates the manufacture, distribution, and sale of various products, including drugs. Among the purposes of the FDCA is to ensure that drugs in the United States are safe and effective, and bear labeling containing only true and accurate information.

9. The FDCA defines the term "drug" to include "articles intended for use in the diagnosis, cure, mitigation, treatment, or prevention of disease in man or other animals...." and "articles intended for use as [components thereof]". 21 U.S.C. § 321(g)(1)(B)&(D).

10. The FDCA defines "labeling" as "all labels and other written, printed or graphic matter (1) upon any article or any of its containers or wrappers, or (2) accompanying such article" 21 U.S.C. § 321(m).

11. Under the FDCA, a drug is deemed to be misbranded if its labeling "is false or misleading in any particular." 21 U.S.C. § 352(a). In addition, a drug is deemed to be misbranded unless its labeling bears adequate directions for use and adequate warnings. 21 U.S.C. § 352(f).

12. The FDA has issued regulations addressing the labeling requirements for active pharmaceutical ingredients (API) used in compounding. *See* 21 C.F.R. 201.120. If an API meets all of the labeling requirements in 21 C.F.R. § 201.120, it is exempt from the statutory requirement under 21 U.S.C. § 352(f) to provide adequate directions for use and the requisite warning information. Pursuant to 21 C.F.R. § 201.120, API used in compounding must bear the statement "for prescription compounding." 21 C.F.R. § 201.120. In addition, if the API, due to its toxicity or other potential for harm, is not safe for use except under the supervision of a licensed practitioner, its labeling must also bear the statement "Rx only." 21 C.F.R. § 201.120(b)(2). However, the exemption established in 21 C.F.R. § 201.120, does not apply to an API intended for use in compounding that results in a new drug unless an approved new drug application covers such use of the drug in compounding prescriptions. 21 C.F.R. § 201.120(c).

13. If API fails to meet the exemption established in 21 C.F.R. § 201.120, then it is misbranded pursuant to 21 U.S.C. § 352(f).

14. Under the FDCA, it is unlawful to introduce (or cause the introduction of) misbranded drugs into interstate commerce. 21 U.S.C. § 331(a). It is also unlawful under the statute to receive a misbranded drug in interstate commerce, and then deliver or proffer delivery of the misbranded drug for pay. 21 U.S.C. § 331(c).

15. The FDCA defines the term "interstate commerce" as the commerce between any State in the United States and any place outside thereof. 21 U.S.C. § 321(b). Thus, when an item is imported into the United States from another country, it is considered to have traveled in interstate commerce under the FDCA.

16. Pursuant to 21 U.S.C. § 333(a)(1), "[a]ny person who violates a provision of [21 U.S.C. § 331 *et seq.*] shall be imprisoned for not more than one year..." and fined in accordance with Title 18. However, any person who commits such a violation with the intent to defraud or mislead, shall be imprisoned for not more than three years. 21 U.S.C. § 333(a)(2).

Smuggling

17. The criminal prohibition on smuggling is established at 18 U.S.C. § 545. Section 545 prohibits, among other things, "fraudulently or knowingly import[ing] or bring[ing] into the United States, any merchandise contrary to law...." 18 U.S.C. § 545. Any person who violates section 545 shall be

imprisoned for not more than twenty years and fined in accordance with Title 18. 18 U.S.C. § 545.

False Declarations

18. Under 18 U.S.C. § 542, it is illegal to introduce merchandise into commerce in the United States "by means of any fraudulent or false invoice, declaration, affidavit, letter, paper, or by means of any false statement, written or verbal, or by means of any false or fraudulent practice or appliance...." 18 U.S.C. § 542. Any person who violates section 542 shall be imprisoned for not more than two years, and fined in accordance with Title 18.

PREMISES TO BE SEARCHED, AND ITEMS SOUGHT

19. Based upon my training and experience, along with my personal knowledge of the facts of the investigation to which this affidavit relates and information obtained from other FDA and Customs and Border Patrol (CBP) employees, I respectfully submit there is probable cause to believe that the business of CBSCHEM LIMITED, located at 621 S. 48th Street, Tempe, Arizona, as more fully described in Attachment A, which is attached hereto and incorporated herein by reference, contains evidence and instrumentalities of violations of federal law by KAMRAN RAZA MALIK and CBSCHEM LIMITED, including Smuggling pursuant to 18 U.S.C. § 545, False Declarations pursuant to 18 U.S.C. § 542 and violations of the FDCA pursuant to 21 U.S.C. §333(a)(1)&(2).

PROBABLE CAUSE

20. CBSCHEM LIMITED is licensed as a pharmaceutical drug wholesaler by the Arizona State Board of Pharmacy. CBSCHEM LIMITED is registered with the Arizona Corporation Commission (ACC) under File Number F-1461534. Its Domestic Address is listed as Unit 1303, 13 Floor, Block 4, Nan Fung, Indust City# 18 TIN, Hau Rd, Tuen Mun, New Territories, Hong Kong and its Foreign Address is listed as 621 S. 48th Street, Suite 114, P.O. Box 7100 Tempe, Arizona (it appears that the company reversed the domestic and foreign addresses). The ACC filing further identifies KAMRAN RAZA MALIK (MALIK) as the Statutory Agent.

21. MALIK has been identified by U.S. Immigration and Customs Enforcement as a Pakistani born foreign national and citizen of Hong Kong.

22. Between October 15, 2011 and October 15, 2012, CBSCHEM LIMITED had been identified by the FDA's Center for Drug Evaluation and Research (CDER) as actively importing misbranded bulk API into the United States from the CBSCHEM LIMITED facility in Hong Kong. Multiple CBSCHEM packages have been detained by U.S. Customs and Border Protection (CBP) and FDA because the drugs were deemed to be misbranded due to the fact that the labeling was false and/or misleading

23. On July 26, 2012, CBP discovered a United States Postal Service Express Mail Parcel (#EA085011721HK) from Hong Kong labeled as containing 20,747 grams of powder. Contained within the parcel were 20 aluminum bags

labeled "Pyrantel Pamoate." Pyrantel Pamoate is an API found in animal drugs used for deworming. CBP tested the substance, confirmed that it was Pyrantel Pamoate and requested further guidance from the FDA regulatory authorities. FDA regulatory authorities determined that the drug was misbranded under the FDCA as there were no adequate directions for use and Pyrantel Pamoate does not qualify for an exemption as it is not intended for use in compounding resulting in a new drug covered by an approved new drug application as further described in the following paragraph.

24. On September 19, 2012, CBP discovered a CBSCHEM LIMITED parcel coming into the United States from Hong Kong that was identified as "Estriol." Estriol is an API found in human drugs used for hormone therapy. The parcel was inspected by Karen Robles, FDA Compliance Officer, who made the following determination: "An API intended for use in pharmacy compounding may be exempt from FDCA section 502(f)(1) [21 U.S.C. § 352(f)(1)] if it meets the conditions outlined in 21 CFR section 201.120. However, pursuant to 21 CFR section 201.120(c), this exemption does not apply to an API intended for use in compounding that results in a new drug unless an approved new drug application covers such use of the drug in compounding prescriptions. Because Estriol is not the subject of such an application, it does not qualify for the exemption and, therefore, **appears misbranded under section 502(f)(1) of the Act [21 U.S.C. §352(f)(1)].** In addition, the **API must be listed as required by section 510(j) of the Federal Food, Drug, and Cosmetic Act (the Act) [21 U.S.C. §360(j)],** the

API must be declared for pharmacy compounding upon importation, and the label must bear the statements required in 21 CFR Part 201. Although the firm is registered and drug listed, it does not in any way denote approval of the firm or its drug. For the reasons cited above, **Estriol API is subject to refusal of admission under section 801(a)(3) of the Act [21 U.S.C. §381(a)(3)],** and CDER supports its detention."

25. On March 14, 2013 Dennis Poertner, FDA Consumer Safety Officer (CSO) in Ontario, California, produced a memorandum and excel spreadsheet identifying 175 CBSCHEM foreign parcel entries known to FDA between October 15, 2011 and October 15, 2012. Of those 175 imports, none of the foreign drug manufacturers reported by CBSCHEM LIMITED possessed a valid Drug Listing Registration as required by the FDA under 21 U.S.C. § 360(i). Therefore all 175 of the CBSCHEM imports would be considered misbranded under 21 U.S.C. § 352(o).

26. On April 24, 2013, Consumer Safety Officers (CSO) Lisa Schultz and Tim Kapsala from the FDA's Tempe Resident Office conducted an inspection of the CBSCHEM LIMITED facility located at 621 S. 48th Street, Tempe, AZ. 85281. The FDA CSO's arrived unannounced and declared their intent to inspect the facility as a function of their normal regulatory duties.

27. During the FDA inspection, CSO Schultz spoke telephonically with MALIK who claimed to be located in Hong Kong. MALIK told CSO Schultz that

all of his company's products are contract manufactured and that all labeling is done by the manufacturers with labeling provided by CBSCHEM. MALIK further stated that all CBSCHEM LIMITED shipments of API are shipped directly to the CBSCHEM LIMITED facility in Tempe that then sells to customers in the United States. MALIK told CSO Schultz that his facilities do not re-label or repackage any manufactured product.

28. CSO Schultz identified one package that had arrived via Federal Express from Hong Kong on the same day. The contents of the package were identified as "Silicone Dioxide" by the accompanying CBSCHEM LIMITED invoice and U.S. Customs Declaration. (Note that Silicone Dioxide is not an API, but is considered to be an inert filler substance for foods and drugs.) Inside the package, Inspectors found seven different APIs, ranging from 1kg to 10 kg each, identified by a number code that was affixed to each of the individual packages. The package did not contain any Silicone Dioxide. Further, Kyle McDonald, a CBSCHEM LIMITED employee, provided the inspectors with an e-mail from MALIK, dated April 24, 2013 at 9:41 a.m. that instructed McDonald to identify and report the individual labeling codes to MALIK. Additionally, MALIK stated in the e-mail that he would send shipping documents to McDonald upon confirmation of the individual labels.

29. A later e-mail, dated April 24, 2013 at 2:41 p.m. from MALIK, identified each of the seven APIs by chemical name and weight and to whom they were to be shipped to for sale.

30. Following the inspection, CSO Schultz contacted me and related the above-stated information. Further, CSO Schultz felt that OCI should become actively involved in the investigation of CBSCHEM LIMITED as she felt that CBSCHEM LIMITED was now engaging in the intentional smuggling of API's to avoid inspection by CBP and FDA of CBSCHEM LIMITED drugs.

31. During the inspection, CBSCHEM LIMITED employees informed CSO Schultz that MALIK kept calling the facility and telling the employees not to say anything to the inspectors regarding the business operations.

32. Further, CSO Schultz related to me that all three employees present during the inspection were upset by the business practices and had immediately resigned following the inspection, leaving the facility unlocked and unattended.

33. On April 25, 2013, I spoke to CBSCHEM LIMITED employee Kelli McDonald. McDonald relayed that there were as many as five laptop computers in the CBSCHEM LIMITED Tempe facility and that most of the business was conducted via internet and e-mail correspondence with MALIK since MALIK spent the majority of his time in Hong Kong.

34. Continuing on April 25, 2013, I spoke telephonically with CBSCHEM LIMITED employee Kyle McDonald. Mr. McDonald told me that, beginning in early March of 2013, he began to receive drug packages from the

CBSCHEM LIMITED office in Hong Kong which were mislabeled. Mr. McDonald stated that the packages were identified as a particular drug or substance on the U.S. Customs declarations and shipping invoices, however, the contents of the parcels were actually multiple undeclared APIs in separate packaging. Mr. McDonald told me that inside the package was a clear plastic bag that was marked with a taped on label identifying the contents as the declared substance. Contained within the plastic bag was an unmarked silver foil package that contained additional smaller silver foil packages. Contained within the smaller packages were clear plastic bags that contained the actual APIs and were either labeled by code or by the actual API name for each product.

35. Following the arrival of each of these packages, Mr. McDonald was contacted by MALIK, usually by e-mail or by internet Instant Messaging. MALIK would give instructions to Mr. McDonald as to how he should identify, re-label and repackage each API for shipment to CBSCHEM LIMITED customers. According to Mr. McDonald, this practice began shortly after MALIK began complaining to his employees that CBSCHEM LIMITED drugs were being detained by CBP and FDA upon entry.

36. Based on the information provided in this Affidavit, it is believed that at least five computers are located at each of the premises to be searched and have been used to communicate with employees and customers of CBSCHEM LIMITED and others.

37. Based on my knowledge and experience, I know that individuals often maintain and utilize computers in their business to connect to the internet, to send, receive and store emails and attachments, and to access, manage, and store bank account and other financial information. Based on my knowledge and experience, I am aware that the individuals often possess and utilize computers or similar devices which contain electronic records.

Technical Terms

38. The following technical terms will be used to convey the following meanings:

39. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static – that is, long-term – IP addresses, while other computers have dynamic – that is, frequently changed – IP addresses.

40. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and

international borders, even when the devices communicating with each other are in the same state.

41. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, floppy disks, flash memory, CD-ROMs, and several other types of magnetic or optical media not listed here.

Computers, Electronic Storage, and Forensic Analysis

42. As described above and in Attachment B, this application seeks permission to search for records that might be found on the premises to be searched, in whatever form they are found. One form in which the records might be found is as electronic data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

43. Probable cause. I submit that if a computer or storage medium is found on the premises to be searched, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience it is known that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a

storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

e. Based on a review of specific email correspondence and attachments to same emails related to this investigation, including Adobe Acrobat ".pdf" files, I believe that computer equipment was used to generate, store, and print documents used in efforts to obstruct the grand jury. As explained above, there is reason to believe that there is a computer system currently located on the premises to be searched.

44. Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer in the premises to be searched because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a

deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and "chat programs" store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to send emails and transmit electronic files in the commission of a crime, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

45. Necessity of seizing or copying entire computers or storage media. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data

recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a

controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

46. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), when persons executing the warrant conclude that it would be impractical to review the media on-site, the warrant I am applying for would permit seizing or imaging storage media that reasonably appear to contain some or all of the evidence described in the warrant, thus permitting its later examination consistent with the warrant. The examination may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

47. The seizure of the computers used for business may limit CBSCHEM's ability to conduct its legitimate business, however as of this application, there are no known employees working at the Tempe facility. As with any search warrant, I expect that this warrant will be executed reasonably. Reasonable execution will likely involve conducting an investigation on the scene of what computers, or storage media, must be seized or copied, and what computers or storage media need not be seized or copied. Where appropriate,

officers will copy data, rather than physically seize computers, to reduce the extent of disruption. If a representative of CBSCHEM LIMITED so requests, the agents will, to the extent practicable, attempt to provide CBSCHEM with copies of data that may be necessary or important to the continuing function of CBSCHEM. If, after inspecting the computers, it is determined that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it.

CONCLUSION

48. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe KAMRAN RAZA MALIK and CBSCHEM LIMITED have been engaged in Smuggling pursuant to 18 U.S.C. § 545, False Declarations pursuant to 18 U.S.C. § 542 as well as violations of the FDCA pursuant to 21 U.S.C. §333(a)(1)&(2).

49. Based on the facts and evidence summarized herein, I respectfully submit there is probable cause to believe that evidence, fruits, and instrumentalities of violations listed in the above paragraph will be found at CBSCHEM LIMITED, as more fully described in Attachment A. I respectfully request that the court issued the proposed search warrant.

Richard C. Langley, Special Agent FDA/OCI

SUBSCRIBED AND SWORN to before me this 26th day of April, 2013.

DAVID K. DUNCAN
United States Magistrate Judge